

# THE VOJTA CONJECTURE IMPLIES GALOIS RIGIDITY IN DYNAMICAL FAMILIES

WADE HINDES

**ABSTRACT.** We show that the Vojta (or Hall-Lang) conjecture implies that the arboreal Galois representations in a 1-parameter family of quadratic polynomials are surjective if and only if they surject onto some finite and uniform quotient. As an application, we use the Vojta conjecture, our uniformity theorem over  $\mathbb{Q}(t)$ , and Hilbert's irreducibility theorem to prove that the prime divisors of many quadratic orbits have density zero.

To prove the surjectivity of the  $\ell$ -adic Galois representation attached to an elliptic curve, it suffices to prove the surjectivity onto some finite quotient. Namely, if  $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$  is a closed subgroup that surjects onto  $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$  for some small  $n$ , then  $G$  must be equal to  $\mathrm{GL}_2(\mathbb{Z}_\ell)$ ; see [17]. However, in [7] Rafe Jones has suggested that such a rigidity is unlikely to hold if we replace  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  with the automorphism group  $\mathrm{Aut}(T_\infty)$  of an infinite binary rooted tree  $T_\infty$ , replace the subgroup  $G$  with the image of an arboreal Galois representation  $G_\infty(\phi)$  attached to a quadratic polynomial  $\phi \in \mathbb{Q}[x]$  (cf. [1] and [8]), and replace  $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$  with the automorphism group  $\mathrm{Aut}(T_n)$  of a level  $n$  binary rooted tree  $T_n$ ; here the difficulty arises from the fact that the Frattini subgroup of  $\mathrm{Aut}(T_\infty)$  has infinite index. To illustrate this point, Jones cleverly constructs a large quadratic polynomial

$$(1) \quad \phi(x) = (x - 88255775491812351975604)^2 + 88255775491812351975605,$$

satisfying  $G_8(\phi) \cong \mathrm{Aut}(T_8)$  and  $G_\infty(\phi) \not\cong \mathrm{Aut}(T_\infty)$ ; see [7]. However, our uniformity theorem over rational function fields (cf. [3, Theorem 1]) together with Hilbert's irreducibility theorem suggest that such a rigidity holds in a 1-parameter family obtained by specializing a quadratic polynomial with polynomial coefficients. In this paper we prove such a claim, assuming some powerful (yet standard) conjectures in arithmetic geometry. As a consequence, we predict that the prime divisors of many quadratic orbits have density zero (cf. Corollary 1).

*Notation:* We fix some notation. Let  $\phi(x) = (x - \gamma(t))^2 + c(t)$  for some polynomials  $\gamma, c \in \mathbb{Z}[t]$  and let  $\phi_a(x) = (x - \gamma(a))^2 + c(a)$  be the specialization of  $\phi$  at some integer  $a$ . Finally, we say that  $\phi_a$  is *stable* if every iterate of  $\phi_a$  is irreducible. Then we have the following theorem regarding the arboreal Galois representations  $G_\infty(\phi_a)$  in the family  $\{\phi_a\}_{a \in \mathbb{Z}}$ .

**Theorem 1.** *Suppose that  $\phi$  is not isotrivial,  $\phi(\gamma) \cdot \phi^2(\gamma) \neq 0$ , and the Vojta (or Hall-Lang) conjecture holds. Then there exists an integer  $n_\phi > 0$  and an effectively computable finite set  $F_\phi$  such that for all integers  $a \notin F_\phi$ ,*

$$G_{n_\phi}(\phi_a) \cong \mathrm{Aut}(T_{n_\phi}) \text{ implies that } G_\infty(\phi_a) \cong \mathrm{Aut}(T_\infty).$$

Furthermore, if  $\phi_a$  is stable, then

$$\sup_{\substack{a \notin F_\phi \\ \phi_a \text{ is stable}}} \left\{ [\mathrm{Aut}(T_\infty) : G_\infty(\phi_a)] \right\} \text{ is finite.}$$

The study of arboreal representations owes its beginnings to classical prime factorization problems in polynomial recurrences. Specifically, let  $\phi \in \mathbb{Z}[x]$  be a polynomial with integer coefficients and let  $b = b_0 \in \mathbb{Z}$ . For  $n \geq 1$ , define the sequence  $b_n = \phi(b_{n-1}) = \phi^n(b_0)$ . A fundamental object in dynamics, this set of numbers is called the *orbit* of  $b$  with respect to  $\phi$  and is denoted

$$(2) \quad \mathcal{O}_\phi(b) := \{b, \phi(b), \phi^2(b), \dots\}.$$

It is a classical question in number theory to ask whether  $\mathcal{O}_\phi(b)$  contains infinitely many primes. At the moment, this question is well beyond reach. For example, if  $\phi(x) = (x-1)^2 + 1$  and  $b = 3$ , then  $b_n = 2^{2^n} + 1$  are the Fermat numbers, which have been studied extensively [10].

However, one can ask a more tractable question, which has connections to arboreal representations. Namely, how big is the set of prime divisors in a particular orbit? As a partial answer, it is known that  $G_\infty(\phi) \cong \text{Aut}(T_\infty(\phi))$  implies that the set

$$(3) \quad \mathcal{P}_\phi(b) := \{\text{primes } p \mid b_n = \phi^n(b) \equiv 0 \pmod{p} \text{ for some } n \geq 1\}$$

of prime divisors of  $\mathcal{O}_\phi(b)$  has density zero [8, Theorem 4.1]. Intuitively, this means that if the Galois groups of iterates of  $\phi$  are as large as possible, then the prime divisors in any particular orbit cannot accumulate. To illustrate this point and Theorem 1, we use our uniformity theorem over  $\mathbb{Q}(t)$  (cf. [3, Theorem 1]) and Hilbert's irreducibility theorem to predict that the prime divisors of many quadratic orbits have density zero.

**Corollary 1.** *Suppose that  $\phi$  satisfies the following conditions:*

- (a)  $\phi$  is not isotrivial
- (b)  $G_{m_\phi}(\phi) \cong \text{Aut}(T_{m_\phi})$  for  $m_\phi$  given by

$$m_\phi := \begin{cases} 17 & , \deg(\gamma) \neq \deg(c) \\ 2 \cdot \log_2 \left( 78 \cdot \frac{\deg(\gamma)}{\deg(c-\gamma)} + 9 \right) & , \deg(\gamma) = \deg(c) \end{cases}.$$

*Then the Vojta (or Hall-Lang) conjecture implies the following statements:*

- (1) *There exists a thin set  $E_\phi$  such that  $G_\infty(\phi_a) \cong \text{Aut}(T_\infty)$  for all  $a \notin E_\phi$ .*
- (2) *The density  $\delta(\mathcal{P}_{\phi_a}(b)) = 0$  for all  $b \in \mathbb{Z}$  and all  $a \notin E_\phi$ .*

Before we begin the proof of the theorem, we remind the reader of the relevant conjectural height bounds in arithmetic geometry. In keeping with standard notation, we let  $h : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$  be the (absolute) logarithmic height of an algebraic number [15, VIII.5]. Similarly, for  $f \in \mathbb{Q}[x]$ , we let  $h(f)$  be the maximum of the heights of the coefficients of  $f$ .

**Conjecture 1.** *For all  $d \geq 3$  there exist constants  $C_1 = C_1(d)$  and  $C_2 = C_2(d)$  so that for all  $f \in \mathbb{Z}[x]$  of degree  $d$  with  $\text{disc}(f) \neq 0$ , if  $x, y \in \mathbb{Z}$  satisfy  $y^2 = f(x)$ , then*

$$(4) \quad h(x) \leq C_1 \cdot h(f) + C_2.$$

*Remark 1.1.* Versions of Conjecture 1 were made by Hall and Lang (cf. [15, IV.7]) for  $d \leq 4$ . On the other hand, for larger  $d$  Conjecture 1 is a consequence of the Vojta conjecture; see the main result of [5] or [16, Example 5].

*Proof (Theorem).* To prove Theorem 1, we need only assume that the bounds in Conjecture 1 hold for a single value of  $d \geq 3$ . Therefore, without loss of generality, we assume that (4) holds for  $d = 3$ . Throughout the proof, we use the following fact: for all  $f \in \mathbb{Q}[x]$  of degree  $d$  there are constants  $\mathcal{C}_{1,f}$  and  $\mathcal{C}_{2,f}$ , depending on  $f$ , such that

$$(5) \quad d \cdot h(\alpha) - \mathcal{C}_{1,f} \leq h(\alpha) \leq d \cdot h(\alpha) + \mathcal{C}_{2,f} \quad \text{for all } \alpha \in \bar{\mathbb{Q}};$$

see [14, Theorem 3.11]. We fix some notation. Define the affine transformation  $\lambda_a(x) = x + \gamma(a)$ , and let  $\sigma_a$  be the quadratic polynomial given by conjugating  $\phi_a$  by  $\lambda_a$ , that is

$$\sigma_a(x) := \lambda_a^{-1} \circ \phi_a \circ \lambda_a(x) = x^2 + c(a) - \gamma(a).$$

The triangle inequality on the absolute values of  $\mathbb{Q}$  and (5) imply that

$$(6) \quad h(\lambda_a^{-1}(\alpha)) \leq h(\alpha) + 2 \cdot \log(3) + \deg(\gamma) \cdot h(a) + h(\gamma) \quad \text{for all } \alpha \in \bar{\mathbb{Q}}.$$

On the other hand, there is a lower bound

$$(7) \quad h(\alpha) - \deg(\gamma) \cdot h(a) - A_{1,\phi} \leq h(\lambda_a^{-1}(\alpha)) \quad \text{for all } \alpha \in \bar{\mathbb{Q}}$$

and some positive constant  $A_{1,\phi}$ ; see [14, Theorem 3.11]. Moreover, repeated application of the triangle inequality implies that

$$(8) \quad h(\sigma_a^m(\alpha)) \leq 2^m \cdot (h(\alpha) + A_{2,\phi} + \deg(c - \gamma) \cdot h(a)) \quad \text{for all } \alpha \in \bar{\mathbb{Q}}$$

and some positive constant  $A_{2,\phi}$ . Finally, since  $\phi$  is not isotrivial,  $\deg(c - \gamma) \neq 0$ . In particular, (5) implies that there exists a computable, positive constant  $B_{1,\phi}$  such that

$$(9) \quad \deg(c - \gamma) \cdot h(a) - B_{1,\phi} \leq h(c(a) - \gamma(a)), \quad \text{for all } a \in \bar{\mathbb{Q}}.$$

From here, we derive Theorem 1 from the following lemma, which ensures the existence of so called square-free, primitive prime divisors in the critical orbit after a uniform number of iterates; compare to [2] and [13].

**Lemma 1.1.** *Assume the Vojta (or Hall-Lang) conjecture and suppose that  $a \in \mathbb{Z}$  satisfies the following properties:*

- (1)  $\phi_a(\gamma(a)) \cdot \phi_a^2(\gamma(a)) \neq 0$ ,
- (2)  $c(a) - \gamma(a) \notin \{-2, -1, 0, \}$ ,
- (3)  $\deg(c - \gamma) \cdot h(a) - B_{1,\phi} > 0$ .

*Then there is an  $n_\phi > 0$  (not depending on  $a$ ) such that for all  $n > n_\phi$  there exists an odd prime  $p_n$  with the following property:*

$$(10) \quad v_{p_n}(\phi_a^n(\gamma(a))) \not\equiv 0 \pmod{2} \quad \text{and} \quad v_{p_n}(\phi_a^j(\gamma(a))) = 0 \quad \text{for all } 1 \leq j \leq n-1;$$

*here  $v_p$  denotes the normalized  $p$ -adic valuation. Such a prime  $p_n$  is called a square-free, primitive prime divisor for  $\phi_a^n(\gamma(a))$ .*

*Proof.* For every  $n$ , write  $\phi_a^n(\gamma(a)) = 2^{e_n} \cdot d_n \cdot y_n^2$  for  $e_n \in \{0, 1\}$  and some odd, square-free integer  $d_n$ . Our goal is to first prove that the  $d_n$  grow rapidly, and from there deduce that eventually each new  $d_n$  is divisible by a new prime. Note that if the  $d_n$ 's were to grow slowly, then (ignoring the power of 2 for now), there would be values of  $d$  for which the curve  $dY^2 = \phi_a^2(X)$  has a rational point with very large coordinates compared to the height of its defining equation. Quantifying this idea leads to a contradiction of Conjecture 1.

If  $n$  is such that no prime  $p_n$  as in (10) exists, then  $d_n$  is a unit or  $d_n = \prod p_i$  for some primes  $p_i \in \mathbb{Z}$  satisfying  $p_i \mid \phi_a^{m_i}(\gamma(a))$  and  $1 \leq m_i \leq n-1$ . On the other hand, if  $d_n$  is not a unit, then each  $p_i \mid \phi_a^{n-m_i}(0)$ , since  $p_i \mid \phi_a^{m_i}(\gamma(a))$  and  $p_i \mid \phi_a^n(\gamma(a))$ . To see this, note that

$$\phi_a^{n-m_i}(0) \equiv \phi_a^{n-m_i}(\phi_a^{m_i}(\gamma(a))) \equiv \phi_a^n(\gamma(a)) \equiv 0 \pmod{p_i}.$$

In particular, when  $d_n$  is not a unit, we have the refinement:

$$(11) \quad d_n = \prod p_i, \quad \text{where } p_i \mid \phi_a^{t_i}(\gamma(a)) \text{ or } p_i \mid \phi_a^{t_i}(0) \quad \text{for some } 1 \leq t_i \leq \left\lfloor \frac{n}{2} \right\rfloor.$$

Our goal is to show that  $n$  is bounded independently of  $a$ . To do this, define the elliptic curve

$$(12) \quad C_{\phi_a}^{(d_n)} : Y^2 = 2^{e_n} \cdot d_n \cdot (X - c(a)) \cdot \phi_a(X).$$

Note that  $C_{\phi_a}^{(d_n)}$  is nonsingular by assumption (1) of Lemma 1.1. Then we have the integral point

$$(13) \quad \left( \phi_a^{n-1}(\gamma(a)), 2^{e_n} \cdot d_n \cdot y_n \cdot (\phi_a^{n-2}(\gamma(a)) - \gamma(a)) \right) \in C_{\phi_a}^{(d_n)}(\mathbb{Z}).$$

In particular, the Hall-Lang conjecture (cf. Conjecture 1 for  $d = 3$ ) on integral points of elliptic curves implies that

$$(14) \quad h(\phi_a^{n-1}(\gamma(a))) \leq \kappa_1 \cdot h(d_n) + \kappa_2 \cdot h(a) + \kappa_3$$

for some absolute constants  $\kappa_i > 0$ .

Assuming the Vojta conjecture, one obtains a similar bound as in (14); we simply replace  $C_{\phi_a}^{(d_n)}$  and the point on (13) with the genus two curve  $Y^2 = 2^{e_n} \cdot d_n \cdot (X - c(a)) \cdot \phi_a^2(X)$  and its corresponding point with  $X$ -coordinate  $\phi_a^{n-2}(\gamma(a))$ ; see [4] for more on these hyperelliptic curves defined by iteration. Finally, apply the main result of [5]; see also [16, Example 5].

Combining (6) and (14), we obtain

$$(15) \quad h(\lambda_a^{-1}(\phi_a^{n-1}(\gamma(a)))) \leq \kappa_1 \cdot h(d_n) + \kappa_{2,\phi} \cdot h(a) + \kappa_{3,\phi},$$

where the constants  $\kappa_{2,\phi}$  and  $\kappa_{3,\phi}$  depend of  $\phi$ . However,

$$\lambda_a^{-1}(\phi_a^{n-1}(\gamma(a))) = \lambda_a^{-1} \circ \phi_a^{n-1} \circ \lambda_a(0) = \sigma_a^{n-1}(0).$$

On the other hand, the canonical height (cf. [14, 3.4]) satisfies

$$|\hat{h}_{\sigma_a}(x) - h(x)| \leq h(c(a) - \gamma(a)) + \log(2) \leq \deg(c - \gamma) \cdot h(a) + B_{1,\phi} + \log(2),$$

for all  $x \in \mathbb{Q}$ ; see [6, Lemma 12]. In particular, we apply this bound to  $x = \sigma_a^{n-1}(0)$  and use (15) to conclude that

$$(16) \quad 2^{n-1} \cdot \hat{h}_{\sigma_a}(0) = \hat{h}_{\sigma_a}(\sigma_a^{n-1}(0)) \leq \kappa_1 \cdot h(d_n) + \kappa'_{2,\phi} \cdot h(a) + \kappa'_{3,\phi}.$$

Moreover, Ingram has shown in [6, Proposition 11], that

$$\hat{h}_{\sigma_a}(x) \geq \frac{1}{32} \max \{h(c(a) - \gamma(a)), 1\}, \quad \text{for all wandering points } x \in \mathbb{Q}.$$

By assumption  $c(a) - \gamma(a) \notin \{-2, -1, 0\}$ , so that 0 is a wandering point of  $\sigma_a$  (equivalently,  $\phi_a$  is not postcritically finite). To see this, note that if 0 is not wandering, then  $c(a) - \gamma(a)$  belongs to the Mandelbrot set  $\mathcal{M}$  over the complex numbers; see [14, §4.24]. In particular, [14, Proposition 4.19] implies that  $|c(a) - \gamma(a)| \leq 2$ , where  $|\cdot|$  denotes the complex absolute value. Hence the absolute logarithmic height of  $c(a) - \gamma(a)$  is at most  $\log(2)$ . One checks that this implies that  $c(a) - \gamma(a) \in \{0, -1, -2\}$  as claimed.

On the other hand, we know there exists a positive constant  $B_{1,\phi}$  as on (9). Consolidating this fact with the lower bound on  $\hat{h}_{\sigma_a}(0)$  and the bound on (16), we obtain that

$$(17) \quad 2^{n-6} \cdot (\deg(c - \gamma) \cdot h(a) - B_{1,\phi}) \leq \kappa_1 \cdot h(d_n) + \kappa'_{2,\phi} \cdot h(a) + \kappa'_{3,\phi}.$$

The left hand side of (17) is of our desired shape. It remains to bound  $h(d_n)$  in terms of  $h(a)$ , to complete the proof of Lemma 1.1. To do this, note that (7) and (11) together imply that

$$(18) \quad \begin{aligned} h(d_n) &\leq \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} h(\phi_a^i(\gamma(a))) + \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} h(\phi_a^j(0)) \\ &\leq \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} h(\sigma_a^i(0)) + \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} h(\sigma_a^j(\gamma(a))) + n \cdot (\deg(\gamma) \cdot h(a) + A_{1,\phi}) \end{aligned}$$

On the other hand, (8) implies that

$$h(\sigma_a^i(0)) \leq 2^i \cdot (A_{2,\phi} + \deg(c-\gamma) \cdot h(a)) \quad \text{and} \quad h(\sigma_a^j(\gamma(a))) \leq 2^j \cdot (h(\gamma(a)) + A_{2,\phi} + \deg(c-\gamma) \cdot h(a)).$$

However, there exists a positive constant  $A_{3,\phi}$ , such that  $h(\gamma(a)) \leq \deg(\gamma) \cdot h(a) + A_{3,\phi}$ . Hence,

$$(19) \quad \begin{aligned} h(d_n) &\leq 2^{\lfloor \frac{n}{2} \rfloor + 2} \cdot (A_{2,\phi} + \deg(c-\gamma) \cdot h(a)) + 2^{\lfloor \frac{n}{2} \rfloor + 1} \cdot (\deg(\gamma) \cdot h(a) + A_{3,\phi}) \\ &\quad + n \cdot (\deg(\gamma) \cdot h(a) + A_{1,\phi}) \end{aligned}$$

Combining (17) and (19), we see that

$$(20) \quad \begin{aligned} 2^{n-6} &\leq \left( \frac{\kappa_1 \cdot \deg(c-\gamma) \cdot h(a) + \kappa_1 \cdot A_{2,\phi}}{\deg(c-\gamma) \cdot h(a) - B_{1,\phi}} \right) \cdot 2^{\lfloor \frac{n}{2} \rfloor + 2} + \left( \frac{\kappa_1 \cdot \deg(\gamma) \cdot h(a) + \kappa_1 \cdot A_{3,\phi}}{\deg(c-\gamma) \cdot h(a) - B_{1,\phi}} \right) \cdot 2^{\lfloor \frac{n}{2} \rfloor + 1} \\ &\quad + \left( \frac{\kappa_1 \cdot \deg(\gamma) \cdot h(a) + \kappa_1 \cdot A_{1,\phi}}{\deg(c-\gamma) \cdot h(a) - B_{1,\phi}} \right) \cdot n + \left( \frac{\kappa'_{2,\phi} \cdot h(a) + \kappa'_{3,\phi}}{\deg(c-\gamma) \cdot h(a) - B_{1,\phi}} \right). \end{aligned}$$

However, as a real valued function, any linear fractional transformations  $\rho(x) = \frac{ax+b}{cx+d}$  is bounded away from its poles. Hence, if we view  $h(a)$  as the variable  $x$ , we see that

$$(21) \quad 2^{n-6} \leq M_{1,\phi} \cdot 2^{\lfloor \frac{n}{2} \rfloor + 2} + M_{2,\phi} \cdot 2^{\lfloor \frac{n}{2} \rfloor + 1} + M_{3,\phi} \cdot n + M_{4,\phi},$$

since  $\deg(c-\gamma) \cdot h(a) - B_{1,\phi} > 0$ . In particular, if  $M_\phi := \max\{M_{i,\phi}\}$ , then

$$(22) \quad n \leq \max\{6, 2 \cdot \log_2(M_\phi) + 19\}.$$

Therefore, we have bounded  $n$  independently of  $a$ . This completes the proof of Lemma 1.1.  $\square$

With the lemma in place, we return to the proof of Theorem 1. Let  $P_\phi(t)$  be the polynomial whose roots cut out conditions (1) and (2) of Lemma 1.1, that is

$$(23) \quad P_\phi(t) := \phi(\gamma(t)) \cdot \phi^2(\gamma(t)) \cdot (c(t) - \gamma(t)) \cdot (c(t) - \gamma(t) + 1) \cdot (c(t) - \gamma(t) + 2).$$

From here, we can define the finite set of exceptional specializations:

$$(24) \quad F_\phi := \left\{ a \in \mathbb{Z} \mid P_\phi(a) = 0 \quad \text{or} \quad h(a) \leq \frac{B_{1,\phi}}{\deg(c-\gamma)} \right\}.$$

*Remark 1.2.* The set  $F_\phi$  can be explicitly computed provided that the Nullstellensatz step in computing  $B_{1,\phi}$  can be carried effectively; see the proof of the lower bound in [14, Proposition 3.11].

We now set  $n_\phi := 1 + \max\{2, 2 \cdot \log_2(M_\phi) + 19\}$  and suppose that  $G_{n_\phi}(\phi_a) \cong \text{Aut}(T_{n_\phi})$  and that  $a \notin F_\phi$ . To prove that  $G_\infty(\phi_a) \cong \text{Aut}(T_\infty)$ , we first show that  $\phi_a$  is stable.

If  $\phi_a$  is not stable, then [9, Proposition 4.2] implies that  $\phi_a^n(\gamma(a))$  is a square for some  $n \geq 1$ . However, by Lemma 1.1, such an  $n$  must be less than  $n_\phi$ . In particular,  $G_{n-1}(\phi_a) \cong \text{Aut}(T_{n-1})$ , as the Galois group of the larger iterate  $\phi_a^{n_\phi}$  is maximal. Moreover, since the full automorphism group of the preimage tree acts transitively on the roots of  $\phi_a^{n-1}$ , we conclude that  $\phi_a^{n-1}$  must be irreducible.

On the other hand, [3, Lemma 1] implies that  $K_n(\phi_a)/K_{n-1}(\phi_a)$  is not maximal, since  $\phi_a^n(\gamma(a))$  is a square in  $K_{n-1}(\phi_a)$ ; in fact, it is already a square over the rational numbers. Therefore,  $G_n(\phi_a) \not\cong \text{Aut}(T_n)$ , contradicting our assumption that  $G_{n_\phi}(\phi_a) \cong \text{Aut}(T_{n_\phi})$ . We conclude that  $\phi_a$  is stable.

Now, let  $m$  be any integer and suppose that the subextension  $K_m(\phi_a)/K_{m-1}(\phi_a)$  is not maximal. In particular,  $m > n_\phi$  since  $G_{n_\phi}(\phi_a) \cong \text{Aut}(T_{n_\phi})$ . However, we have shown that  $\phi_a$  is stable, hence  $\phi_a^m(\gamma(a)) \in (K_{m-1}(\phi_a))^2$ ; see [3, Lemma 1]. Hence, if we write  $\phi_a^m(\gamma(a)) = 2^{e_m} \cdot d_m \cdot y_m^2$  for some  $y_m, d_m \in \mathbb{Z}$  such that  $d_m$  is a unit or an odd square-free integer, then the primes dividing  $d_m$  must ramify in  $K_{m-1}(\phi_a)$ .

On the other hand, by [11, Corollary 2, p.159], we see that the primes which ramify in  $K_{m-1}$  must divide the discriminant of  $\phi^{m-1}$ . Let  $\Delta_n$  be the discriminant of  $\phi^n$ . Then we have the following formula, given in [9, Lemma 2.6]:

$$(25) \quad \Delta_n = \pm \Delta_{n-1}^2 \cdot 2^{2^n} \cdot \phi^n(\gamma).$$

In particular, if  $d_m$  is not a unit, then  $d_m = \prod p_i$  for some odd primes  $p_i \in \mathbb{Z}$  such that  $p_i | \phi^{m_i}(\gamma)$  and  $1 \leq m_i \leq m-1$ . However, since  $m > n_\phi$ , Lemma 1.1 implies that there exists a prime divisor of  $d_m$  which is coprime to all lower iterates, a contradiction. Hence,  $K_m(\phi_a)/K_{m-1}(\phi_a)$  is maximal for all  $m$ . It follows that  $G_\infty(\phi_a) \cong \text{Aut}(T_\infty)$ , completing the first statement of the Theorem 1.

Similarly, if  $a \notin F_\phi$  and  $\phi_a$  is stable, then Lemma 1.1 implies that the subextensions  $K_m(\phi_a)/K_{m-1}(\phi_a)$  are maximal for all  $m > n_\phi$ . Hence  $G_\infty(\phi_a)$  is a finite index subgroup of  $\text{Aut}(T_\infty)$ , and

$$[\text{Aut}(T_\infty) : G_\infty(\phi_a)] = [\text{Aut}(T_{n_\phi}) : G_{n_\phi}(\phi_a)] = \frac{2^{2^{n_\phi}-1}}{[K_{n_\phi}(\phi_a) : \mathbb{Q}]} \leq \frac{2^{2^{n_\phi}-1}}{2^{n_\phi}} = 2^{2^{n_\phi}-n_\phi-1},$$

since  $\phi_a^{n_\phi}$  is an irreducible polynomial of degree  $2^{n_\phi}$  over the rational numbers. In particular, the index bound does not depend on  $a$ , which completes the proof of the theorem.  $\square$

If we fix  $\phi$ , it is natural to ask to what extent the corresponding  $n_\phi$  is computable (at least conjecturally). However, since the constants appearing in Conjecture 1 are not explicit, we cannot make the proof of Theorem 1 effective. Nonetheless, it is possible to use additional techniques in the theory of rational points on curves to classify the Galois behavior of small iterates and produce a conjectural  $n_\phi$ . For instance, we make the following conjecture when  $\phi(x) = x^2 + t$ .

**Conjecture 2.** *If  $\phi_a(x) = x^2 + a$ , then for all  $a \in \mathbb{Z}$ ,*

$$G_3(\phi_a) \cong \text{Aut}(T_3) \text{ implies that } G_\infty(\phi_a) \cong \text{Aut}(T_\infty).$$

*In particular, if  $a \neq 3$ , then  $G_2(\phi_a) \cong \text{Aut}(T_2)$  implies that  $G_\infty(\phi_a) \cong \text{Aut}(T_\infty)$ .*

**Remark 1.3.** The evidence for Conjecture 2 comes from [4, Theorem 1.1]. There we prove that  $G_3(\phi_a) \cong \text{Aut}(T_3)$  implies  $G_4(\phi_a) \cong \text{Aut}(T_4)$ . Furthermore, we show that if  $a \neq 3$  and  $G_2(\phi_a) \cong \text{Aut}(T_2)$ , then  $G_4(\phi_a) \cong \text{Aut}(T_4)$ .

We close with the proof of Corollary 1.

*Proof (Corollary).* If  $\phi$  is not isotrivial and  $G_{m_\phi}(\phi) \cong \text{Aut}(T_{m_\phi})$ , then it follows from [3, Theorem 1] that  $G_\infty(\phi) \cong \text{Aut}(T_\infty)$ . In particular,  $\phi(\gamma) \cdot \phi^2(\gamma) \neq 0$  and there exists a finite set  $F_\phi$  and an integer  $n_\phi$  such that

$$(26) \quad G_{n_\phi}(\phi_a) \cong \text{Aut}(T_{n_\phi}) \text{ implies that } G_\infty(\phi_a) \cong \text{Aut}(T_\infty),$$

for all  $a \notin F_\phi$ ; see Theorem 1 above. On the other hand, since  $G_\infty(\phi) \cong \text{Aut}(T_\infty)$ , we conclude that  $G_{n_\phi}(\phi) \cong \text{Aut}(T_{n_\phi})$  and Hilbert's irreducibility theorem implies that the set

$$(27) \quad Z_\phi := \{a \in \mathbb{Z} \mid G_{n_\phi}(\phi_a) \not\cong \text{Aut}(T_{n_\phi})\}$$

is thin; see [12, Theorem 3.4.1]. Hence, the set  $E_\phi := Z_\phi \cap F_\phi$  is also thin, and if  $a \notin E_\phi$ , then (26) and (27) imply that  $G_\infty(\phi_a) \cong \text{Aut}(T_\infty)$ . In particular, the density  $\delta(\mathcal{P}_{\phi_a}(b))$  of prime divisors of  $\mathcal{O}_{\phi_a}(b)$  is zero; see [8, Theorem 4.1]. This completes the proof of Corollary 1.  $\square$

**Acknowledgements:** It is a pleasure to thank Joe Silverman for the many discussions related to the work in this paper. I also thank Michael Stoll for relaying to me the question of Odoni regarding the existence of the thin set  $E_\phi$  for the family  $\phi_a(x) = x^2 + a$  (cf. Corollary 1).

## References

- [1] N. Boston and R. Jones, *The image of an arboreal Galois representation*. Pure and Applied Mathematics Quarterly 5(1) (Special Issue: in honor of Jean-Pierre Serre, Part 2 of 2): 213-225, (2009).
- [2] C. Gratton, K. Nguyen, and T. Tucker. *ABC implies primitive prime divisors in arithmetic dynamics*. Bull. London Math. Soc. 45: 1194-1208, (2013).
- [3] W. Hindes, *Galois uniformity in quadratic dynamics over  $k(t)$* , J. Number Theory, in press, arXiv:1405.0630, (2014).
- [4] W. Hindes, *The arithmetic of curves defined by iteration*. Acta Arith., in press, arXiv:1305.0222, (2014).
- [5] Su-Ion Ih, *Height uniformity for algebraic points on curves*, Compositio Math, 134: 35-57, (2002).
- [6] P. Ingram, *Lower bounds on the canonical height associated to the morphism  $\Phi(z) = z^d + c$* , Monatshefte für Mathematik, 157(1):69-89, (2009).
- [7] R-Jones, *An iterative construction of irreducible polynomials that are reducible modulo every prime*. J. of Algebra 369: 114-128, (2012).
- [8] R. Jones, *Galois representations from pre-image trees: an arboreal survey*, Pub. Math. Besancon, 107-136, (2013).
- [9] R. Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*. J. Lond. Math. Soc. 78.(2): 523-544, (2008).
- [10] M. Krizek, F. Luca, and L. Somer, *17 lectures on Fermat numbers: from number theory to geometry*, Springer, 2001.
- [11] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*. Springer, (2004).
- [12] J-P. Serre, *Topics in Galois theory*. Research Notes in Mathematics 1, Jones and Bartlett Publishers, (1992).
- [13] J. Silverman, *Primitive prime divisors, dynamical Zsigmondy sets, and Vojta's conjecture*. J. Number Theory, 133: 2948-2963, (2013).
- [14] J. Silverman, *The arithmetic of dynamical systems*, Vol. 241, Springer, (2007).
- [15] J. Silverman, *Arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer-Verlag, GTM 106, 1986. Expanded 2nd Edition, (2009).
- [16] M. Stoll, *Rational points on curves*, J. Théor. Nombres Bordeaux 23(1): 257-277, (2011).
- [17] A. Vasiu. *Surjectivity criteria for  $p$ -adic representations, Part I*, Manuscripta Mathematica 112(3): 325-355, (2003).